HIPAA

Administrative Simplification:

Privacy of Individually Identifiable Health Information

The Basics

Rules

- Electronic Transactions & Code Sets (Oct. 2003)
- ***Privacy*** (April 2003)
- Security (draft)
- Identifiers (Providers, Plans, Employers, Individuals?)
- Enforcement (?)

Scope: Applicability

- Covered Entities
  - Health care providers who choose to conduct covered transactions electronically
  - Health plans
  - Health care clearinghouses (translation)
- Business Associates (contractual)
  - Performs a function for or on behalf of a covered entity
  - *and*
  - Receives Protected Health Information from a covered entity

Topics

The Privacy Rule

- **Current Status**
- **Key Concepts**
  - Use and Disclosure
  - Individual Rights
- **Core Requirements**
  - Organizational
  - Administrative

Current Status

Compliance Timeline

- December 28, 2000 - published in *Federal Register*
- April 14, 2001 - rule becomes effective
- April 14, 2003 - compliance date (extra year for small health plans)
  - The recent extension given to implement the transactions and code sets rule does not apply to the privacy rule
- Rule modifications March 27, 2002
  - No release date yet for the new “final” language

Current Status

Enforcement

Office of Civil Rights (DHHS)

Receive and investigate complaints
Conduct compliance reviews

Covered entities must

Provide records and compliance report
Cooperate with investigations and reviews

Enforcement regulations

?

Current Status

Responsibilities of Covered Entities

No enforcement rule yet, but current final rules require covered entities to:

- Keep record and submit compliance reports as determined by the Secretary
- Cooperate with the Secretary
- Permit access to records by Secretary
- Certify what efforts have been made to obtain required information from others

Current Status

Statutory Penalties

Civil penalties

- $100 per violation
- Annual cap: Total penalties not to exceed $25,000 per year for all violations of a single requirement or prohibition

Criminal penalties

- Wrongful disclosure — up to $5,000 and/or 1 year jail time
- False pretenses — up to $100,000 and/or 5 yrs imprisonment
- For profit/with malice — up to $250,000 and/or 10 yrs in jail

Key Concepts

Security vs. Privacy

- Security rules deal with how electronic data is stored, transmitted and accessed.
- Privacy rules deal with how an entity's workforce and agent(s) behaves when using or disclosing the data.

Key Concepts

Preemption of Contrary State Law, but...

- More stringent state laws will prevail
  - Tighter restrictions on use and disclosure
  - More patient control over their information
- Other exemptions from HIPAA preemption:
  - State provisions providing for reporting of disease, injury, child abuse, birth, death, public health surveillance, public health investigations or interventions
  - State law requires health plans to report or provide access to information for management and financial audits, program monitoring or the licensure or certification of facilities or individuals

HIPAA: Administrative Simplification: The Basics

Privacy of Individually Identifiable Health Information

Key Concepts

Preemption of Contrary State Law, unless...

HHS Secretary determines State law is necessary

(A)

- to prevent fraud and abuse*
- to regulate insurance and health plans*
- for reporting of state health care delivery and costs*
- for public health, safety or welfare & determines that privacy intrusion is warranted

or

(B)

- has as its principal purpose the regulation of controlled substances*

HIPAA: Administrative Simplification: The Basics

Privacy of Individually Identifiable Health Information

Key Concepts

Health Information

- Any information (oral or recorded in any form)
  - Created/received by health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse; and
  - Relates to
    - Past, present or future physical or mental health or condition
    - Provision of health care or
    - Past, present or future payment for health care

Key Concepts

Individually Identifiable Health Information

- A subset of health information

  - Past, present or future physical or mental health or condition
  - Provision of health care or
  - Past, present or future payment for health care

  - Created/received by provider, plan, employer ….

- *Individually identifiable or there is a reasonable basis to believe the information can be used to identify the individual*

Key Concepts

Protected Health Information

Individually Identifiable Health Information that is:

Transmitted by electronic media;
Maintained in any electronic medium; or
Transmitted or maintained in any other form or medium

- Any other form or medium means:

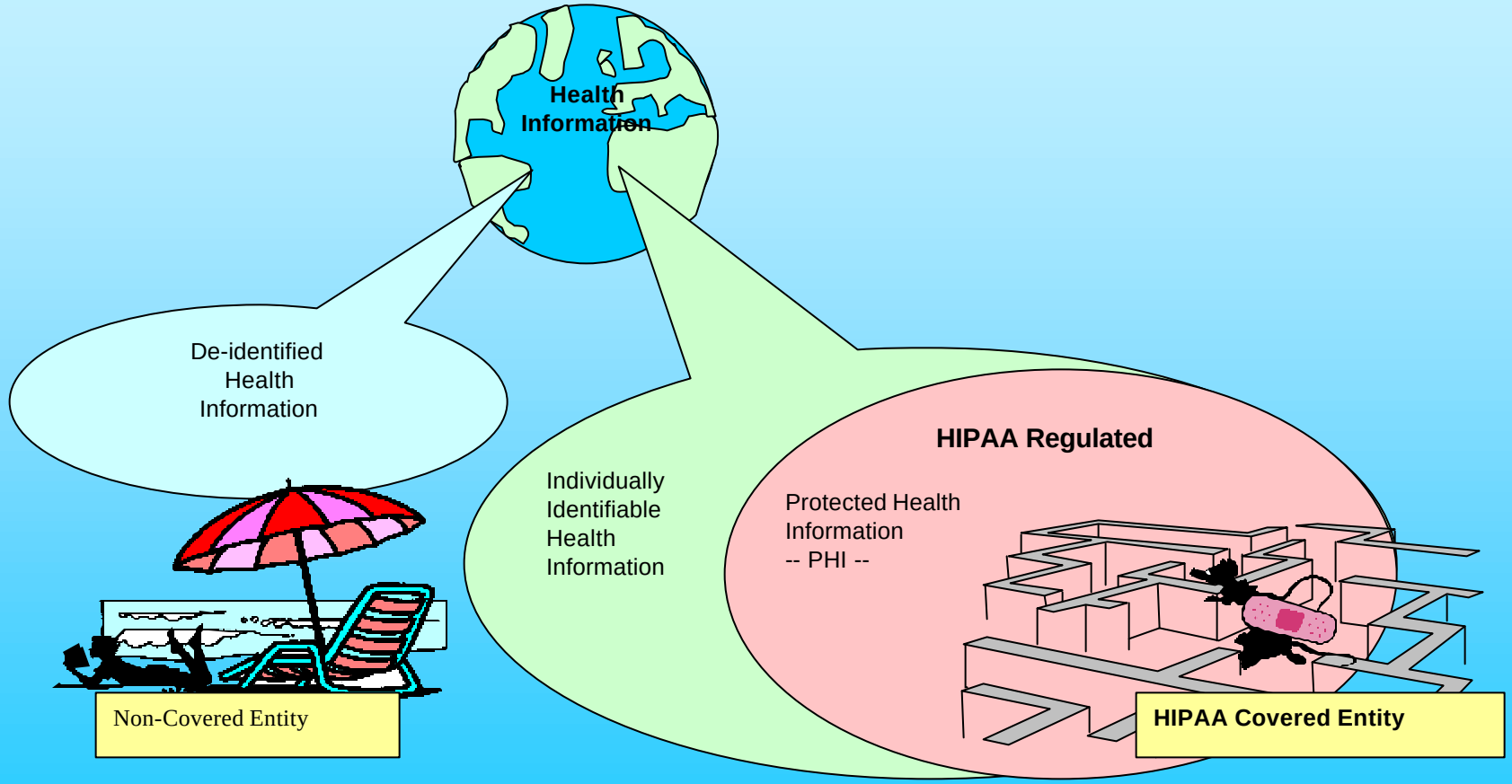
Written
Verbal
Evolving forms of data capture and transmission not comprehended by the definition of "electronic"

HIPAA: Administrative Simplification: The Basics

Privacy of Individually Identifiable Health Information

Key Concepts

HIPAA Regulated Information



Use and Disclosure

- *Use*

  With respect to individually identifiable health information, the sharing, employment, application, utilization, examination, or analysis of such information *within* an entity that maintains such information.

- *Disclosure*

  The release, transfer, provision of access to, or divulging in any other manner of information *outside* the entity holding the information.

Use and Disclosure

Requirements

A covered entity may not use or disclose protected health information, except as permitted or required.

Permitted:

- To the individual who is the subject of the information
- Basically anything an individual "permits" through
  - "Consent"
  - Other agreement
  - "Authorization"
- Exceptions for specified situations

Use and Disclosure

Individual Permissions

Permission Type	Applies to	Requirements
Consent	For treatment, payment and health care operations	- Obtained by direct treatment provider - May condition care upon receiving
Opportunity to Agree/Object	- Facility directories available for inquiry - Notification of others	- Verbal agreement OK - Then document
Authorization	- Everything Else	- Written - Specific Content - Treatment may Not be conditioned on receipt - Revocable

Use and Disclosure

Permitted Exceptions

Permitted exceptions not needing an individual's "permission":

- Required by law
- Public health
- Reports to government authorities of abuse, neglect or domestic violence
- Law enforcement
- Judicial and administrative proceedings
- Health oversight activities
- Avert imminent threat to health or safety of a person or public
- Specialized government functions
- worker's compensation
- Organ donation or transplantation
- Coroners and medical examiners

HIPAA: Administrative Simplification: The Basics

Privacy of Individually Identifiable Health Information

Use and Disclosure

Required

- To individual upon the individual's request
  notable exceptions:
  - ongoing civil, criminal, administrative proceedings
  - inmate's request
  - psychotherapy notes
  - as required by law
- To individual's request for an accounting of disclosures
  notable exceptions:
  - treatment, payment, operations
  - persons involved in care
  - correctional institutions or law enforcement
- To HHS in connection with its enforcement and compliance reviews

Use and Disclosure

Minimum Necessary

Amount of information (PHI) disclosed is restricted to the minimum amount necessary to accomplish intended purpose

- Must make "reasonable efforts" to limit:
  - Identify persons or classes of persons in workforce needing access
  - Identify the category(s) of PHI to which access is needed
  - limit access to those identified and the respective PHI
- Policies and procedures for recurring and routine disclosures

Use and Disclosure

Minimum Necessary

- **Exceptions:**

  - Disclosure among providers for treatment

  - Release authorized by or for individual's own review

  - Disclosure to HHS

  - Compliance with HIPAA requirements

  - Required by law

Individual Rights

- Right to Notice of Privacy Practices
- Right to Access
- Right to Amend
- Right to an Accounting of Disclosures
- Right to request restriction of use and disclosure
- Right to request to receive communications by alternative means or location

Individual Rights

Right to Notice of Privacy Practices

- Be written in plain language with example(s) of permitted use and disclosure
- Describe purposes not needing consent or authorization
- Describe more stringent use and disclosure law
- Include a statements regarding:
  - individual rights to access, inspection, accounting
  - covered entities duties
  - complaints and contacts
  - effective date
- An inmate does not have a right to notice under HIPAA

Individual Rights

Provision of Notice

Health Plan

At time of enrollment

Within 60 days of a revision

Not less than every three years

Provider

No later than date of first service delivery

Have available for pick-up

Post in a clear and prominent location

When revised, make available on revision effective date

Individual Rights

Right to Access and Amend

Right to access own PHI

- Inspect and copy for as long as PHI is maintained
- Provide access in form or format requested
- Summary of information if individual agrees in advance
- Some exclusions
- Other -- denying access

Right to amend own PHI

- Accepting amendment
  - Inform individual & amend
  - Distribute to prior recipients
- Denying amendment
  - Not created by covered entity
  - Covered entity believes PHI is accurate and complete
  - Denial letter, statement of disagreement, rebuttal

HIPAA: Administrative Simplification: The Basics

Privacy of Individually Identifiable Health Information

Individual Rights

Right to Receive an Accounting of Disclosures

- Covered entity accounts for disclosures in the six years prior to request
  - Date and purpose of disclosure
  - Recipient name and address
  - Description of information disclosed
  - Statement of the purpose of the disclosure
  - Provide accounting within 60 days of request
  - Document above + titles or offices processing requests
- Exceptions:
  - Treatment, payment and health care operations
  - To the individual or those involved in care
  - Facility directories
  - Correctional institutions,
  - Health oversight or law enforcement agencies if impedes activities

    Temporary suspension - no longer than 30 days

Individual Rights

Other Rights

Right to request restriction of use and disclosure

- Includes treatment, payment, health care operations
- Covered entity may refuse
- If agrees → bound (except for emergency treatment)

Right to request to receive communications by alternative means or location

- Correspondence sent to alternate address
- Alternative means of communication
- Must permit request and accommodate reasonable requests
  - Health Plan must accommodate if individual endangered may require statement to that effect
  - Provider may not require explanation
- Covered entity may require written request

HIPAA: Administrative Simplification: The Basics

Privacy of Individually Identifiable Health Information

Organizational Impacts

- Consent
- Authorizations
- Minimum Necessary
- Business Associates
- De-Identifying Protected Health Information

Organizational Impacts

Consent

- Required for providers, optional for health plans
- Individual's "consent," prior to use or disclosure, for treatment, payment or health care operations
- May condition treatment/enrollment on consent
- Exceptions:
  - Emergency treatment situations
  - Care required by law but unable to obtain consent (after attempt)
  - Providers with "indirect relationship" to patient
  - Inmates of correctional facilities
  - Substantial communication barriers with inferred consent

Organizational Impacts

Consent: Specifications

- Content
  - Use and disclose for treatment, payment and operations
  - Refer to notice of privacy practices
  - Rights to request limitations or revoke consent
  - Signed and dated by individual
- Can be brief and written in general terms
- Must document failure to obtain consent and reasons
- Defective consent = no consent
- Joint consents for organized health care arrangement

Organizational Impacts

Authorization

- If not otherwise permitted, must obtain individual's "authorization" for use or disclosure
- A customized document giving permission to use specified PHI for specified purposes
  - May NOT condition treatment on authorization (except clinical trials)
  - covers only the uses and disclosures stipulated
  - Individual may revoke at any time
  - Applies to all covered entities, not just providers
- *Must* be obtained for any use or disclosure of psychotherapy notes with few exceptions

Organizational Impacts

Authorization: Specifications

- Required elements:
  - Specific description of information
  - Persons authorized to disclose
  - Persons to whom disclosure may be made
  - Right to revoke
  - Information subject to redisclosure
  - Signature and date
  - Expiration date
- Given for specific period of time
- Plain language
- Defective authorization is not valid

Organizational Impacts

Minimum Necessary

Amount of information (PHI) disclosed is restricted to the minimum amount necessary to accomplish intended purpose

- Must make "reasonable efforts" to limit uses:
  - Identify persons or classes of persons in workforce needing access
  - Identify the category(s) of PHI to which access is needed
  - limit access to those identified and the respective PHI
- Policies and procedures for recurring and routine disclosures
- Must have process to review non-routine requests on a case-by-case basis
- Must also abide by any agreed upon restrictions requested by the individual

Organizational Impacts

Minimum Necessary

- **Impact considerations:**

  - Non-treatment uses and disclosures;
    "reasonableness" of Phone, fax, e-mail

  - Applications:
    reports, user screens and e-forms, integrated databases

  - Justifying release of entire medical record - explicitly stated in policy

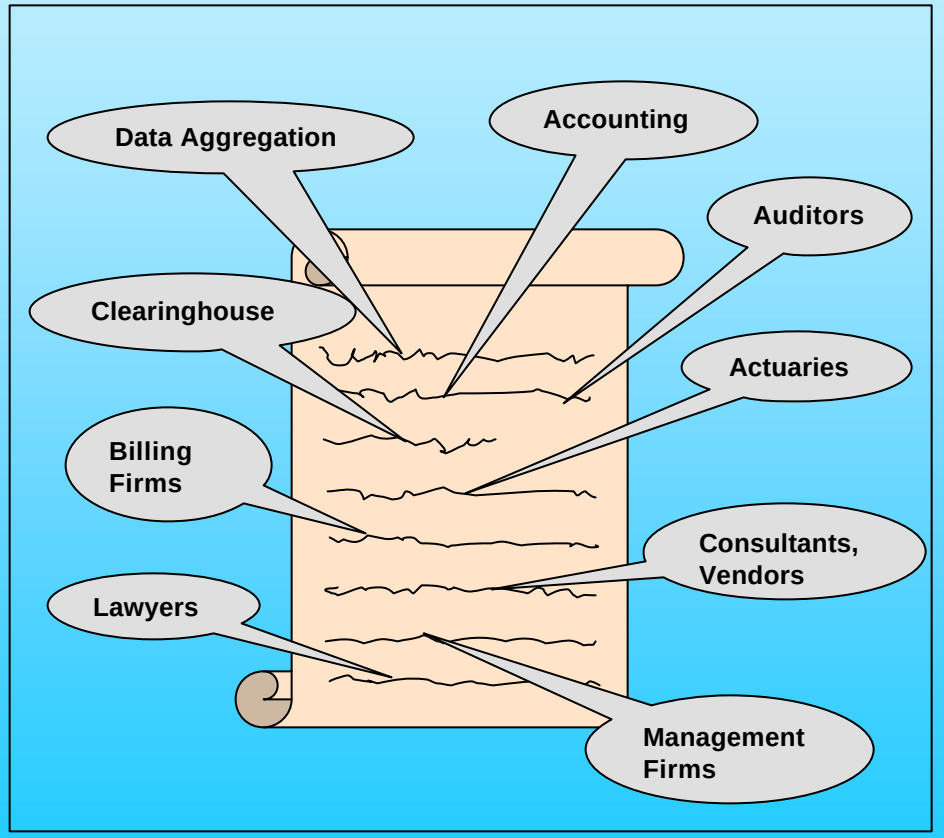
  - Case by case review of non-standard requests

Organizational Impacts

Business Associates

A person who, on behalf of a covered entity - -

- Performs or assists with a function or activity involving:
  - Individually identifiable information, or
  - Otherwise covered by HIPAA
- Performs certain identified services



Organizational Impacts

Business Associates

- Satisfactory Assurances:
  - "Assurance" received through contracts between business associates and covered entity
  - Covered entity need not monitor or oversee means by which business associates carry out contract
- If a violation known to the covered entity:
  - Must take reasonable steps to cure
  - If unsuccessful, must terminate contract
  - If not feasible to terminate, must report to DHHS
  - Otherwise, considered violation by covered entity

Organizational Impacts

De-identified PHI

Use and disclosure restrictions do not apply to de-identified information

- Does not identify an individual (and no key to re-identify may be disclosed)

Covered entity may determine not individually identifiable only by:

(1) a person knowledgeable in statistical and scientific principles determines that there is no reason to believe recipient could identify individual alone or in combination with other information

Or

(2) The safe harbor approach: Removal of all specific identifiers (18), such as:

Names of person, relatives, employers
Address, phone number, fax, email
Social security, plan, account, record numbers

Admin Impacts

Administrative Requirements

- *Implement administrative, technical and physical safeguards*
  - Legal entities with health care components must prevent disclosure to other components not otherwise permitted if they were separate and distinct legal entities
  - must work in tandem with "minimum necessary"
- *Implement policies and procedures to comply with HIPAA*
  - "minimum necessary" coverage for routine disclosures
  - change as necessary to comply with changes in the law
- *Documentation:*
  - all policies and procedures
  - all written communications
  - all required actions
  - all personnel designations
  - maintain for six years

Admin Impacts

Administrative Requirements

Workforce Training and Sanctions

- Training in organization's HIPAA-related PHI policies for:

  - Entire workforce by compliance date
  - New employees following hire
  - Affected employees after material changes in policies

- Privacy and security awareness training to be appropriate for workforce to carry out their functions within the covered entity

- Documentation that training has been provided

Admin Impacts

Administrative Requirements

Additionally, covered entities must:

Complaints --------- Provide a complaint process for individuals

Sanctions ---------- Apply workforce sanctions

Mitigation ---------- Mitigate harmful effects of improper use or disclosure

Retaliation ---------- May not threaten, intimidate, coerce against those exercising rights

Waiver of Rights -- Not require individuals to waive rights

Privacy Official ---- Must designate privacy official and contact person

BA Contracts ------ Must establish permitted uses and disclosures

Summary

- Change in *status quo*
- Very unlike Y2K:
  - Not only an IT issue — mostly business operations, people & processes
  - No endpoint — progresses from planning to implementation to ongoing compliance
- Balancing act:
  - Compliance obligations with organizational size & capabilities
  - Process improvement opportunities with implementation costs

HIPAA: Administrative Simplification: The Basics

Privacy of Individually Identifiable Health Information

What needs to be done?

1. Make basic decisions
   - Confirm covered status
   - Determine what type of organization you are
     (e.g., single covered entity, hybrid organization, etc.)

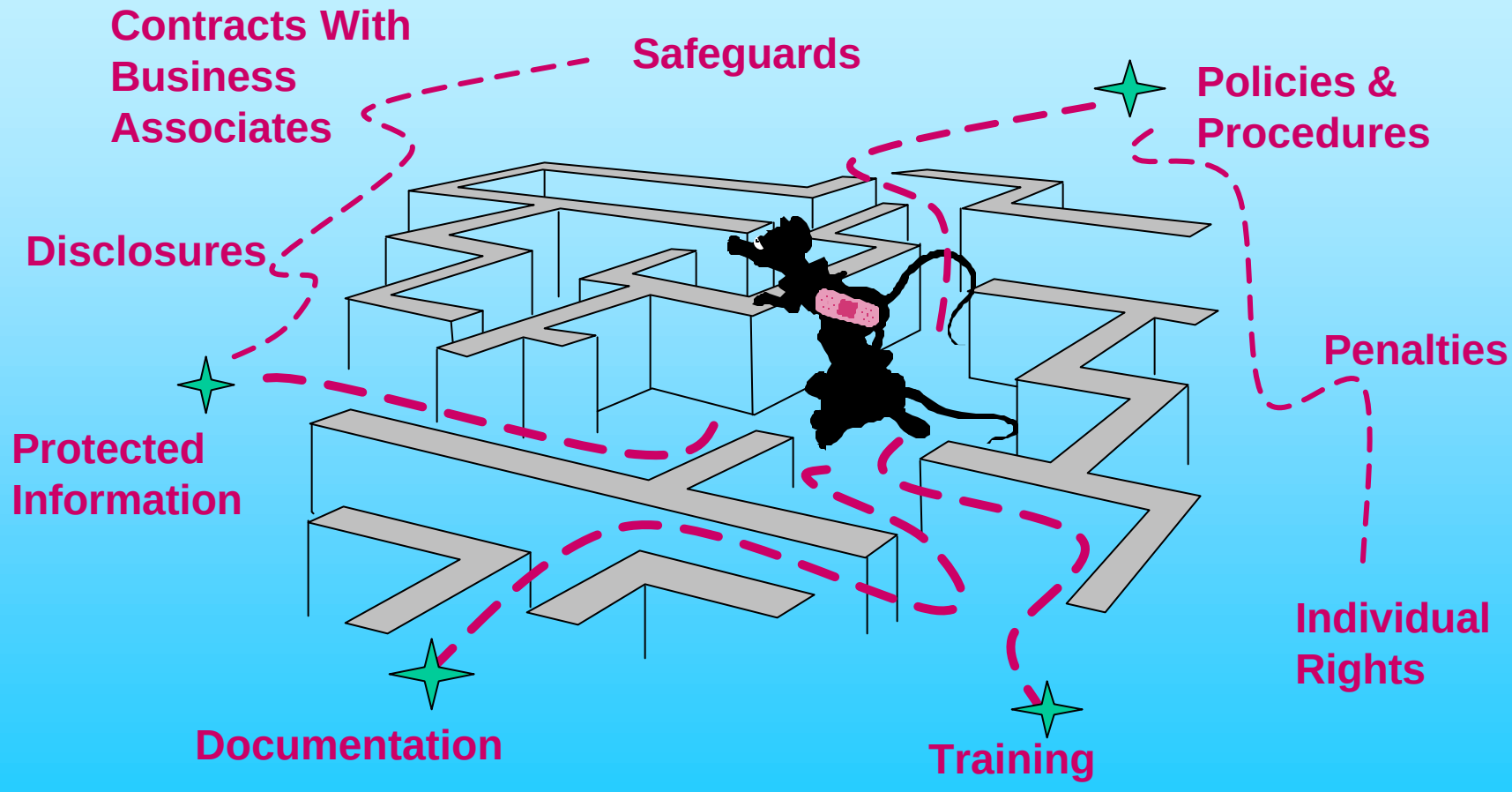
2. Begin planning an initial privacy analyses work effort to identify what specific requirements apply your operations.
   - Identify gaps between those requirements and current practice

3. Utilize the above analysis to develop an action plan to achieve compliance.

4. Decide how to implement the privacy officer function

5. Involve the decision makers
   - Lots of policy level decisions

Action Planning



Next Steps

Privacy Action Plan Considerations

- Assemble project team
- Plan the work effort
  - Internal or external
  - Tools and methodology
- Identify:
  - Where exceptions apply
  - Where HIPAA imposes new requirements
- Determine what needs changing:
  - contracts
  - notice, consent
  - authorizations
  - uses
  - disclosures
  - training
  - policies
  - procedures
  - access, amendment

Next Steps

Don't forget … Proposed Revisions

- No required consent
- Incidental disclosures with reasonable safeguards
- Excludes health information in employment records
- Eases disclosure for payment and operations

Security

But what about the Security Rule?

- No final rule yet
  - current scope is electronic data
- Not a “One size fits all” rule
- Best Practices Approach
- Does not require specific technologies
- Administrative rigor and due diligence

Security

The Proposed Security Rule

Another gap analysis?

Yes. There is a requirement to do an assessment of your current practices and the rule requirements.

"An applications and data criticality analysis (an entity's formal assessment of the sensitivity, vulnerabilities, and security of its programs and information it receives, manipulates, stores, and/or transmits)."

Security

Security: Addendum 1

- Administrative Procedures
- Physical Safeguards
- Technical Security Services
- Technical Security Mechanisms
- Electronic Signatures

Next Steps

Last but not least ...

- Apply for an extension for transaction rule compliance
- Proceed with HIPAA implementations in accordance with legal advisory opinions.
- Proceed with appointing a privacy officer.
  - Define duties and responsibilities
  - Determine organizational placement
- Gain an initial sense of how big your security gap may be.

HIPAA Resources

- Copies of this presentation:
  - The DHFS "HIPAA NOW" web site
    - www.dhfs.state.wi.us/hipaa
    - Click on HIPAA Happenings
- Other sites or resources
  - Click on Helpful Links

Questions?

Contact:

Ted Ohlswager:
phone: (608) 266-5314
e-mail: ohlswts@dhfs.state.wi.us

Rich Ruby:
phone: (608) 267-9044
e-mail: rubyra@dhfs.state.wi.us